

PRUEBA DE HABILIDADES PRÁCTICAS CCNA  
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE  
SOLUCIONES INTEGRADAS LAN / WAN)

LUIS EDUARDO ARMESTO ECHAVEZ  
CÓDIGO: 91421481

Tutor:  
Ing. Juan Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
PROGRAMA INGENIERÍA ELECTRÓNICA  
DIPLOMADO DE PROFUNDIZACIÓN CISCO  
2018

## Dedicatoria

La realización de este trabajo final lo se lo dedico primeramente a Dios, por darme la oportunidad y sobre todo la vida de poder afrontar de manera física este proyecto de estudio, enriqueciéndome minutos a minutos mi vida de bendiciones y poniendo en mis manos todas las fuerzas necesarias, para poder escalar un peldaño más en mi vida... y hacer realidad ese sueño rico en conocimientos.

A mi esposa y a mis hijos por brindarme el espacio de sus vidas ese tiempo que muchas veces por cuestión de trabajo y estudio, frente a esa herramienta quien fuera mi cómplice “el computador”, les robe las horas de disfrutar el tiempo con ellos.

A mis padres y hermanos que a la distancia me brindaron el apoyo necesario para no desfallecer y continuar adelante, de igual manera a esos maestros que dieron lo mejor de ellos “El saber” muchas gracias....

## CONTENIDO

|     |                             |    |
|-----|-----------------------------|----|
| 1.  | AGRADECIMIENTO.....         | 4  |
| 2.  | INTRODUCCIÓN.....           | 5  |
| 3.  | JUSTIFICACIÓN.....          | 6  |
| 4.  | GLOSARIO.....               | 7  |
| 5.  | OBJETIVO GENERAL .....      | 8  |
| 5.1 | Objetivos específicos ..... | 8  |
| 6.  | ESCENARIO 1 .....           | 9  |
| 7.  | ESCENARIO 2.....            | 29 |
| 8.  | CONCLUSIONES.....           | 46 |

## 1. AGRADECIMIENTO

En esta etapa que estoy a punto de culminar quiero extender mis agradecimientos al cuerpo de docentes que durante el paso de la universidad estuvieron siempre conmigo apoyando esta iniciativa de querer emprender un recorrido lleno de mucha satisfacción y poder encaminarme en esta hermosa profesión como es la Ingeniería Electrónica.

Muchas gracias a ustedes por su paciencia y por darme siempre lo mejor de las orientaciones y ánimo de continuar cuando muchas veces quise caer, pero ustedes me tomaron de la mano y me ayudaron a levantarme y continuar el camino. Hoy con orgullo puedo decir que soy el reflejo de ustedes, porque en cada una de las materias encontré un amigo a darme lo mejor de ustedes como es el saber. Gracias a todos por brindarme esa riqueza y en especial a las ingenieras Martha Fabiola Contreras y Julieth Ching Contreras.

## 2. INTRODUCCIÓN

Por medio del presente trabajo denominado Evaluación – Prueba de habilidades CCNA el cual hace parte de la etapa final del diplomado de profundización CISCO, se busca dar solución a dos escenarios específicamente diferentes propuestos el cual se realizará la configuración de cada uno de los dispositivos que comprende el diseño físico, la ejecución de los diferentes comandos de programación para la verificación de su conectividad. Con base en la utilización de recursos y herramientas que se trabajaron en función de los protocolos y soporte de las comunicaciones por medio de las redes de datos, generando soluciones a problemas de conectividad. Completamente independientes entre sí. Donde pondremos a prueba nuestros conocimientos que aprendimos durante el curso.

Sobre cada uno de los escenarios que se resuelven dentro del presente informe se abordan técnicas básicas de la configuración de una red en la cual para que su funcionamiento sea óptimo y estable se hacen uso de comandos para cada uno de los dispositivos necesarios en la red como los son Router, Switch, servidores, computadores entre otros que son necesarios para lograr un buen enrutamiento dentro de la red correspondiente. Para que cada uno de los dispositivos anteriores tengan una buena comunicación dentro de su red es necesario hacer uso del comando correspondiente a cada uno de los dispositivos como lo son: Vlans, configuraciones OSPF, implementación de los protocolos DHCP – NAT y su respectiva verificación de los ACL.

Gracias a la herramienta Packet Tracer, se pudo llevar a cabo nuestro diseño de configuración de una red de manera virtual, haciendo uso de la simulación del Software, logrando entablar comunicación entre router, switch, Servidor y pc. Teniendo en cuenta que de esta manera la universidad puede brindarle al estudiante una enseñanza de manera virtual, donde el estudiante puede llevar a cabo sus proyectos de los diferentes tipos de redes a la realidad por medio de una simulación y sobretodo con la guía del tutor.

### 3. JUSTIFICACIÓN

En esta actividad se busca que el estudiante matriculado en la materia de DIPLOMADO DE PROFUNDIZACIÓN CISCO- UNAD, en la evaluación denominada “Prueba de habilidades prácticas” teniendo en cuenta que para la realización de esta actividad consta de dos escenarios, como es el escenario 1 y escenario 2. Teniendo en cuenta que se busca es que el estudiante demuestre las habilidades adquiridas durante el curso CCNA nivel 1 denominado aspectos básicos del Networking, y para el curso CCNA nivel 2 denominado conceptos y protocolos de enrutamiento.

Es necesario contar con una herramienta muy importante que nos brinda la universidad donde podemos desarrollar los ejercicios propuestos de manera virtual como es el **PACKET TRACER, GNS3**. Y con ello se pretende desarrollar todos los escenarios propuesto para este diplomado de profundización, aplicando los diferentes comandos vistos durante el curso.

#### 4. GLOSARIO

- Conectividad: es la capacidad de un dispositivo de conectarse con otro dispositivo de una forma autónoma.
- Dirección IP: es un direccionamiento utilizado para identificar un dispositivo en la red.
- DNS: (sistema de nombres de dominio) es la nomenclatura utilizada para asociar información de dominio y la dirección IP de cada uno de los dispositivos que conforman o acceden a una red.
- OSPF: protocolo de enrutamiento desarrollado para redes IP, de tipo enlace-estado.
- Ping: comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.
- Protocolos de enrutamiento: conjunto de reglas que permiten determinar la mejor ruta para enviar paquetes de datos entre routers.
- Puertos troncales: enlace punto a punto para enviar y recibir el tráfico entre routers o switches.
- DHCP: (Protocolo de configuración dinámica de host) de tipo cliente/servidor en el que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.
- Protocolo con el cual se intercambian o transportan paquetes entre dos redes normalmente incompatibles.
- Topología física: disposición de cada uno de los dispositivos o hardware dentro de una red.

## 5. OBJETIVO GENERAL

- Dar solución al escenario propuesto como trabajo final del diplomado de profundización CCNA, desarrollando cada uno de los conocimientos adquiridos sobre la implementación y diseño de la topología física y lógica de una red.

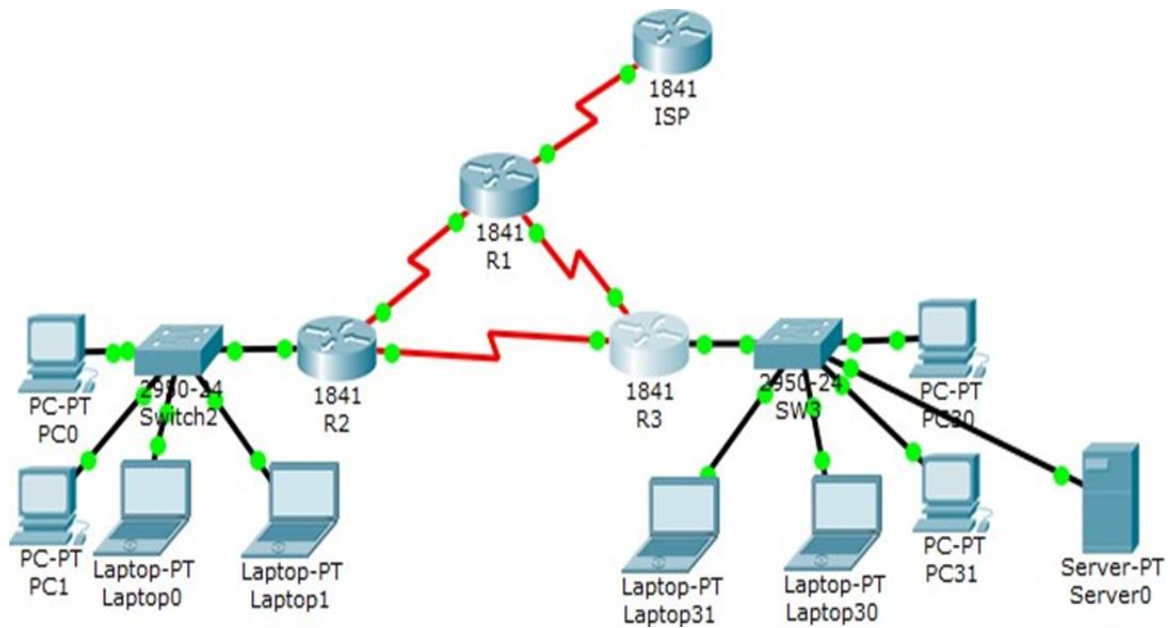
### 5.1 Objetivos específicos

- Analizar la arquitectura propuesta con el fin de implementar su simulación por medio del software Packet Tracer.
- Realizar la Configuración e interconectar entre sí cada uno de los dispositivos que forman parte del escenario propuesto de acuerdo con los protocolos establecidos para el diseño de una topología de red.
- Configuración de los parámetros básicos, DHCP, Nat en Router por medio iOS.

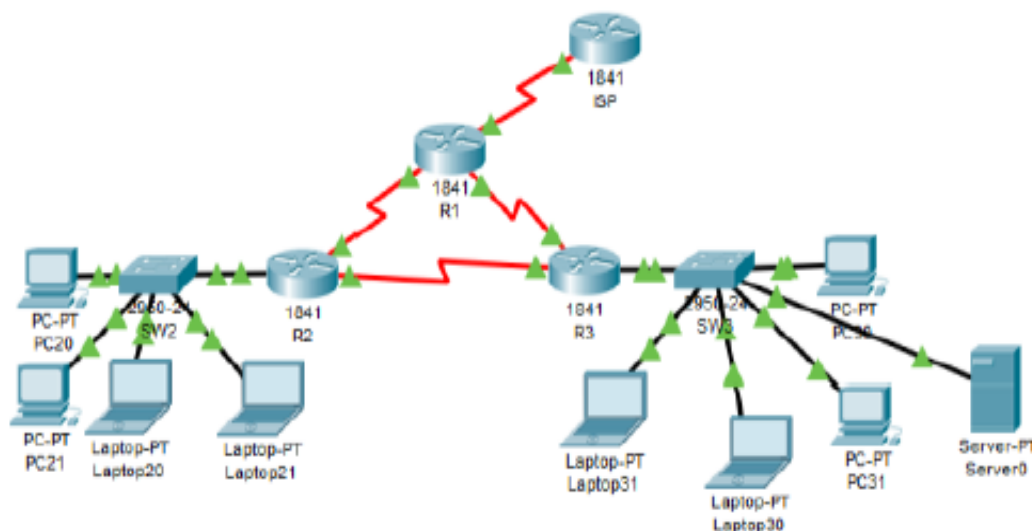


## 6. ESCENARIO 1

Descripción: En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente.



## Topología diseñada Escenario 1



## DESARROLLO DE TRABAJO

### DESCRIPCIÓN

Para la realización de este escenario 1 como parte fundamental es necesario contar con la herramienta PACKET TRACER, que nos permite llevar a cabo de una manera virtual el desarrollo del trabajo y que nos permite manejar diversos comandos de configuración de Router, Switchet, PC, Laptop, dándole así asignaciones a los diferentes puertos de Vlan.

Primero configuramos los routers abriendo sus puertos de conexión y luego los Switchers, teniendo un servidor que está dispuesto y diseñado para mandar la señal de Internet a través de los routers y este a su vez es conectado por los Switcher a los diferentes Laptop y PC. Cada router tiene una tabla de direccionamiento que indica los puertos de conexión de las interfaces con diferentes direcciones IP y su máscara de subred. Teniendo en cuenta todos estos pasos vemos cómo se van dando las interconexiones.

## TABLA DE DIRECCIONAMIENTO

| El administrador | Interfaces | Dirección IP              | Máscara de subred | Gateway predeterminado |
|------------------|------------|---------------------------|-------------------|------------------------|
| ISP              | S0/0/0     | 200.123.211.1             | 255.255.255.0     | N/D                    |
| R1               | Se0/0/0    | 200.123.211.2             | 255.255.255.0     | N/D                    |
|                  | Se0/1/0    | 10.0.0.1                  | 255.255.255.252   | N/D                    |
|                  | Se0/1/1    | 10.0.0.5                  | 255.255.255.252   | N/D                    |
| R2               | Fa0/0,100  | 192.168.20.1              | 255.255.255.0     | N/D                    |
|                  | Fa0/0,200  | 192.168.21.1              | 255.255.255.0     | N/D                    |
|                  | Se0/0/0    | 10.0.0.2                  | 255.255.255.252   | N/D                    |
|                  | Se0/0/1    | 10.0.0.9                  | 255.255.255.252   | N/D                    |
| R3               | Fa0/0      | 192.168.30.1              | 255.255.255.0     | N/D                    |
|                  |            | 2001:db8:130::9C0:80F:301 | /64               | N/D                    |
|                  | Se0/0/0    | 10.0.0.6                  | 255.255.255.252   | N/D                    |
|                  | Se0/0/1    | 10.0.0.10                 | 255.255.255.252   | N/D                    |
| SW2              | VLAN 100   | N/D                       | N/D               | N/D                    |
|                  | VLAN 200   | N/D                       | N/D               | N/D                    |
| SW3              | VLAN1      | N/D                       | N/D               | N/D                    |

|          |     |      |      |      |
|----------|-----|------|------|------|
| PC20     | NIC | DHCP | DHCP | DHCP |
| PC21     | NIC | DHCP | DHCP | DHCP |
| PC30     | NIC | DHCP | DHCP | DHCP |
| PC31     | NIC | DHCP | DHCP | DHCP |
| Laptop20 | NIC | DHCP | DHCP | DHCP |
| Laptop21 | NIC | DHCP | DHCP | DHCP |
| Laptop30 | NIC | DHCP | DHCP | DHCP |
| Laptop31 | NIC | DHCP | DHCP | DHCP |

## Tabla de asignación de VLAN y puertos

| Dispositivo | VLAN | Nombre  | Interfaz             |
|-------------|------|---------|----------------------|
| SW2         | 100  | LAPTOPS | Fa0/2-3              |
| SW2         | 200  | DESTOPS | Fa0/4-5              |
| SW3         | 1    | -       | Todas las interfaces |

Tabla de enlaces troncales

| <b>Dispositivo local</b> | <b><u>Interfaz</u><br/>local</b> | <b>Dispositivo remoto</b> |
|--------------------------|----------------------------------|---------------------------|
| SW2                      | Fa0/2-3                          | 100                       |

6.1 Desarrollo del escenario 1. SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1

SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.

**Para el SW2**

```
enable
config t
vlan 100
name LAPTOPS
vlan 200
name DESTOPS
interface range f0/2-3
switchport mode access
switchport access vlan 100
interface range f0/4-5
switchport mode access
switchport access vlan 200
interface f0/1
switchport mode trunk
```

**Para el SW3**

```
enable
config t
```

```
vlan 1
interface range f0/1-24
switchport mode access
switchport access vlan 1
no shutdown
```

6.2 Los puertos de red que no se utilizan se deben deshabilitar.

```
interface range f0/6-24
shutdown
```

6.3 La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

**Para R2**

```
enable
config t
interface f0/0.100
encapsulation dot1Q 100
ip address 192.168.20.1 255.255.255.0
interface fastEthernet0/0.200
encapsulation dot1Q 200
ip address 192.168.21.1 255.255.255.0
interface fastEthernet0/0
no shutdown
interface serial 0/0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
interface serial 0/0/1
ip address 10.0.0.9 255.255.255.252
```

no shutdown

Para R1

enable

config t

interface serial 0/0/0

ip address 200.123.211.2 255.255.255.0

no shutdown

interface serial 0/1/0

ip address 10.0.0.1 255.255.255.252

no shutdown

interface serial 0/1/1

ip address 10.0.0.5 255.255.255.252

no shutdown

### **Para R3**

enable

config t

ipv6 unicast-routing

interface fastEthernet0/0

ip address 192.168.30.1 255.255.255.0

ipv6 address 2001:db8:130::9C0:80F:301/64

no shutdown

ipv6 dhcp server vlan\_1

ipv6 nd other-config-flag

no shutdown

```
interface serial 0/0/0
ip address 10.0.0.6 255.255.255.252
no shutdown

interface serial 0/0/1
ip address 10.0.0.10 255.255.255.252
no shutdown
```

6.4 Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.

### **Para R2**

```
enable
config t
ip dhcp pool vlan_100
network 192.168.20.1 255.255.255.0
default-router 192.168.20.1

ip dhcp pool VLAN_200
network 192.168.21.1 255.255.255.0
default-router 192.168.21.1

exit
```

### **Para R3**

```
enable
config t
ip dhcp pool vlan_1
network 192.168.30.1 255.255.255.0
default-router 192.168.30.1

ipv6 dhcp pool vlan_1
```

```
dns-server 2001:db8:130::
```

```
exit
```

6.5 R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.

```
enable
```

```
config t
```

```
pool INSIDE-DEVS 200.123.211.2 200.123.211.128 netmask 255.255.255.0
```

```
access-list 1 permit 192.168.0.0 0.0.255.255
```

```
access-list 1 permit 10.0.0.0 0.0.0.255
```

```
ip nat inside source list 1 interface s0/0/0 overload
```

```
interface s0/1/0
```

```
ip nat inside
```

```
interface s0/1/1
```

```
ip nat inside
```

```
interface s0/0/0
```

```
ip nat outside
```

```
ping
```



**Figura 3. NAT con sobrecarga R1**

```
%LINK-S-CHANGED: Interface Serial0/1/1, changed state to up
%LINK-S-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/0,
changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/1,
changed state to up

Router>ping 200.123.211.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.123.211.1, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/6/11 ms
Router>
```

6.6 R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.

```
enable
config t
router r
version 2
router rip
version 2
network 10.0.0.0
default-information originate
ip route 0.0.0.0 0.0.0.0 serial 0/0/0
exit
```

6.7 R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

```
config t
```

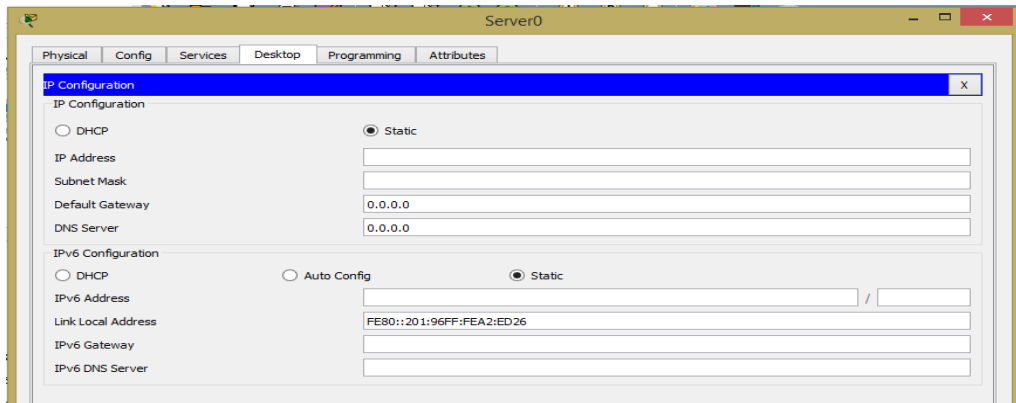
```
router rip
version 2
network 192.168.20.0
network 192.168.21.0
network 192.168.30.0
```

6.8 R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

```
enable
config t
ip dhcp pool vlan_100
network 192.168.20.1 255.255.255.0
default-router 192.168.20.1
ip dhcp pool VLAN_200
network 192.168.21.1 255.255.255.0
default-router 192.168.21.1
exit
```

6.9 El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).

**Imagen # 4. Servidor IPv6 accesible – 1**

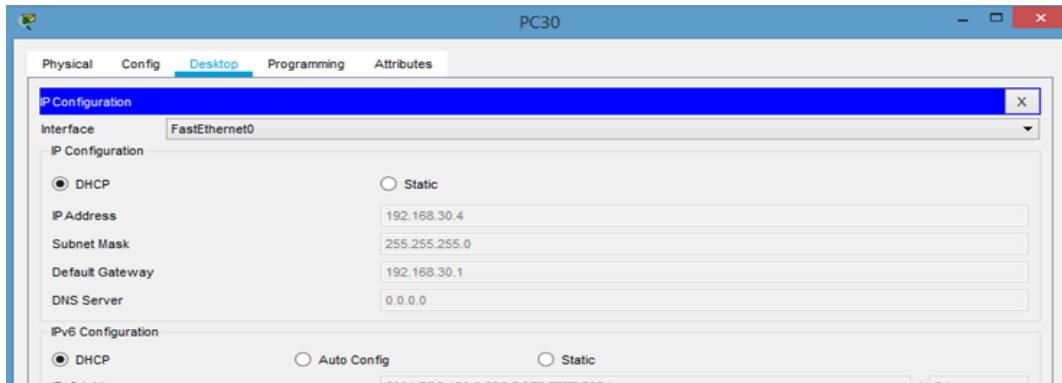


**Imagen # 5. Servidor IPv6 accesible – 2**

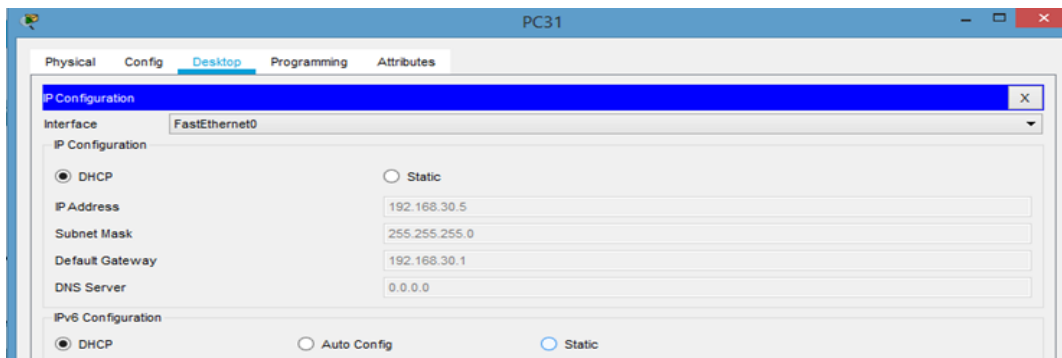
| Realtime Simulation |             |         |             |      |       |           |          |     |        |          |
|---------------------|-------------|---------|-------------|------|-------|-----------|----------|-----|--------|----------|
|                     | Last Status | Source  | Destination | Type | Color | Time(sec) | Periodic | Num | Edit   | Delete   |
|                     | Successful  | PC31    | Server0     | ICMP |       | 0.000     | N        | 0   | (edit) | (delete) |
|                     | Successful  | PC31    | R3          | ICMP |       | 0.000     | N        | 1   | (edit) | (delete) |
|                     | Successful  | PC31    | ISP         | ICMP |       | 0.000     | N        | 2   | (edit) | (delete) |
|                     | Successful  | Server0 | ISP         | ICMP |       | 0.000     | N        | 3   | (edit) | (delete) |

6.10 La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.

## PC 30



## PC 31



## R3

Router>enable

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R3

R3(config)#ipv6 unicast-routing

R3(config)#int f0/0

R3(config-if)#ipv6 enable

R3(config-if)#ip add 192.168.30.1 255.255.255.0

R3(config-if)#ipv6 add 2001:db8::9C0:80F:301/64

R3(config-if)#no shut

R3(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

## **R1**

Router>enable

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#do show ip route connected

C 10.0.0.0/30 is directly connected, Serial10/1/ 0

C 10.0.0.4/30 is directly connected, Serial10/1/ 1

C 200.123.211.0/24 is directly connected, Serial10/0/ 0

R1(config-router)#network 10.0.0.0

R1(config-router)#network 10.0.0.4

R1(config-router)#end

R1#

%SYS-5-CONFIG\_I: Configured from console by console

R1#wr

Building configuration...

[OK]

R1#

**R2**

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R2

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 10.0.0.0

R2(config-router)#network 10.0.0.0

R2(config-router)#network 10.0.0.8

R2(config-router)#do show ip route connected

C 10.0.0.0/30 is directly connected, Serial10/0/ 0

C 10.0.0.8/30 is directly connected, Serial10/0/ 1

C 192.168.20.0/24 is directly connected, Serial10/0/ 0

R2(config-router)#end

R2#

%SYS-5-CONFIG\_I: Configured from console by console

R2#wr

Building configuration...

[OK]

6.11 La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

```
enable
config t
interface fastEthernet 0/0
ip address 192.168.30.1 255.255.255.0
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:130::9C0:80F:301/64
ipv6 nd other-config-flag
ipv6 dhcp server vlan_1
exit
ip access-list extended SERVER
```

6.12 R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

### **Para R1**

```
enable
config t
router rip
version 2
ip route 0.0.0.0 0.0.0.0 s0/0/0
router rip
version 2
network 10.0.0.4
network 10.0.0.0
```

default-information originate

### **Para R2**

enable

config t

router rip

version 2

network 192.168.30.0

network 192.168.20.0

network 192.168.21.0

network 10.0.0.0

network 10.0.0.8

### **Para R3**

enable

config t

router rip

version 2

network 192.168.0.0

network 10.0.0.8

network 10.0.0.4

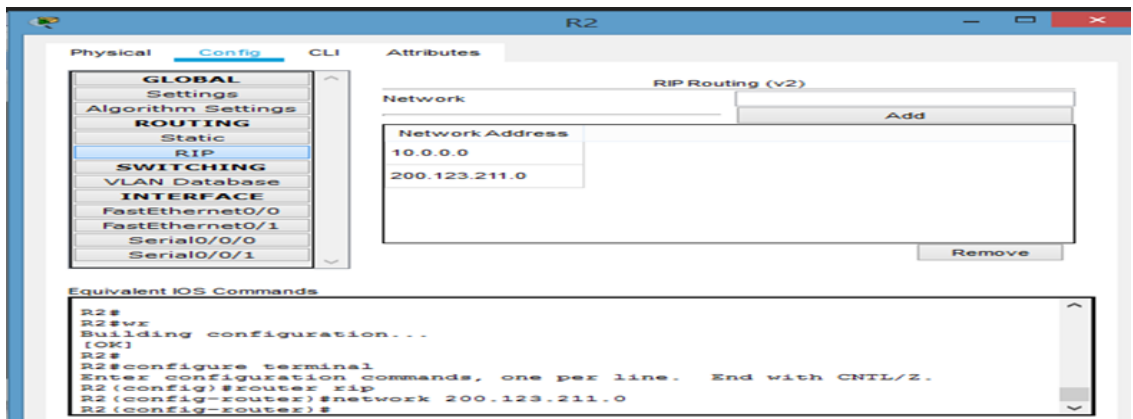
6.13 R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.



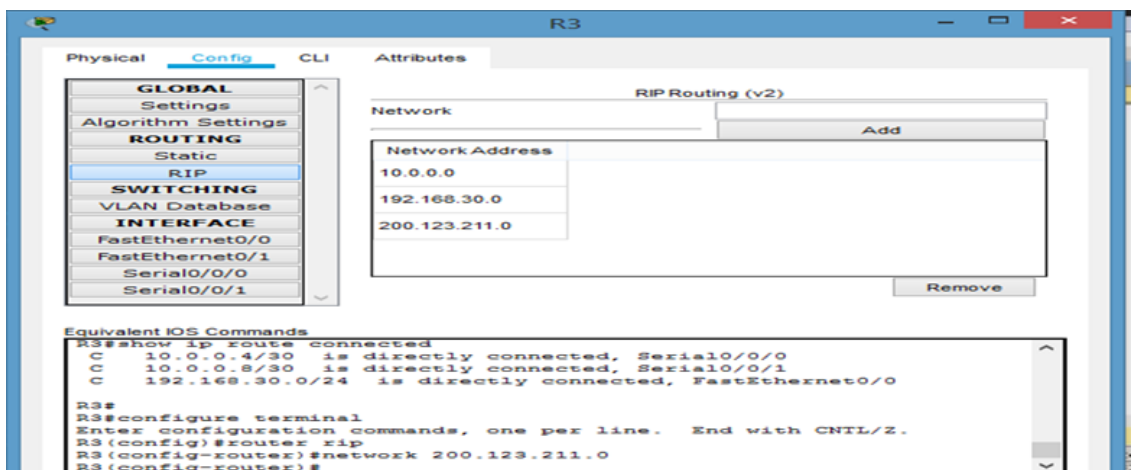
## Para R1



## Para R2

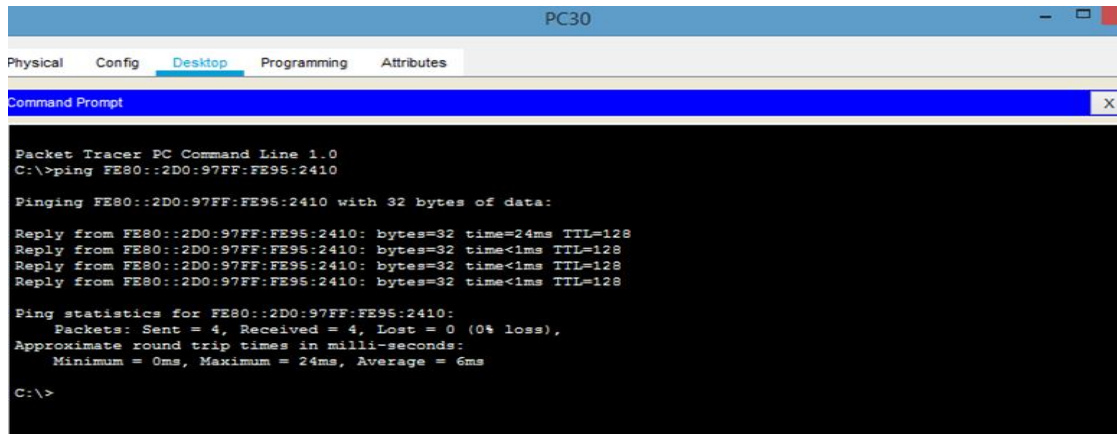


## Para R3



6.14 Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

### Para PC 30



```
PC30
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping FE80::2D0:97FF:FE95:2410

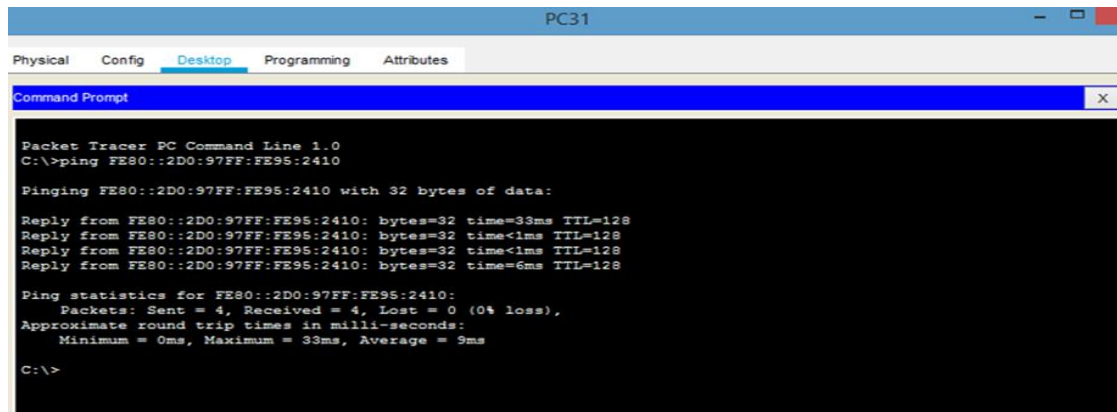
Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:

Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=24ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128

Ping statistics for FE80::2D0:97FF:FE95:2410:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 24ms, Average = 6ms

C:\>
```

### Para PC 31



```
PC31
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping FE80::2D0:97FF:FE95:2410

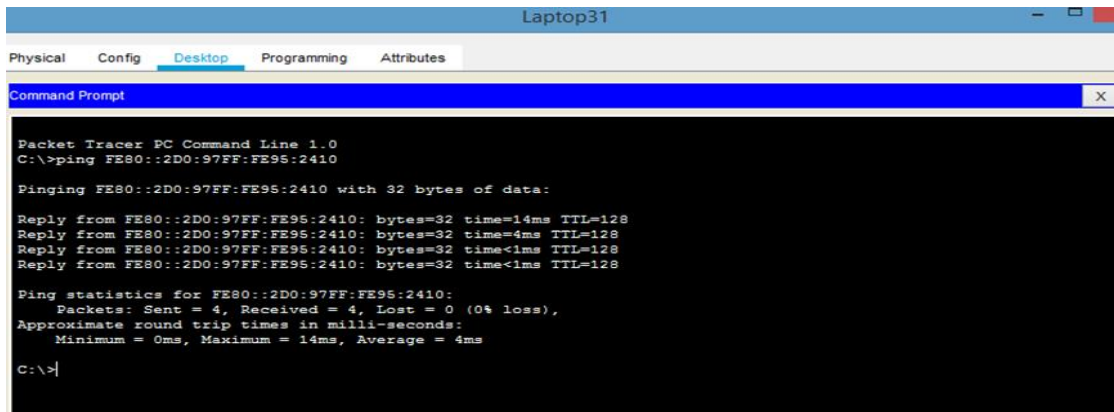
Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:

Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=33ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=6ms TTL=128

Ping statistics for FE80::2D0:97FF:FE95:2410:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 33ms, Average = 9ms

C:\>
```

## Para laptop 31



The screenshot shows the 'Desktop' tab of a Packet Tracer laptop named 'Laptop31'. A command prompt window is open, displaying the execution of a ping command. The command is 'C:\>ping FE80::2D0:97FF:FE95:2410'. The output shows four successful replies from the target address, each with 32 bytes of data, a time of 14ms, and a TTL of 128. The ping statistics indicate that 4 packets were sent, 4 were received, and 0 were lost (0% loss). The approximate round trip times are: Minimum = 0ms, Maximum = 14ms, Average = 4ms.

```
Packet Tracer PC Command Line 1.0
C:\>ping FE80::2D0:97FF:FE95:2410

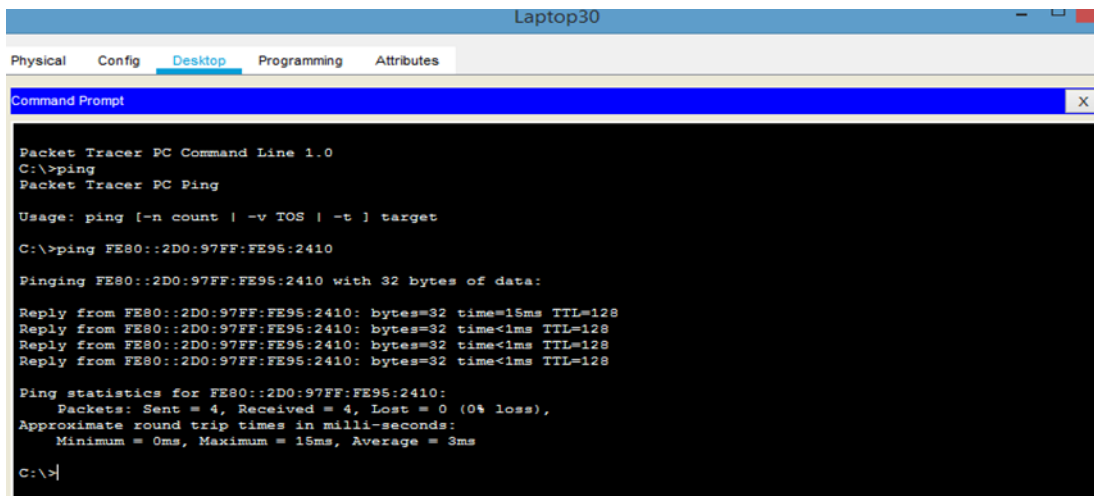
Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:

Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=14ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=4ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128

Ping statistics for FE80::2D0:97FF:FE95:2410:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 4ms

C:\>|
```

## Para laptop 30



The screenshot shows the 'Desktop' tab of a Packet Tracer laptop named 'Laptop30'. A command prompt window is open, displaying the execution of a ping command. The command is 'C:\>ping FE80::2D0:97FF:FE95:2410'. The output shows four successful replies from the target address, each with 32 bytes of data, a time of 15ms, and a TTL of 128. The ping statistics indicate that 4 packets were sent, 4 were received, and 0 were lost (0% loss). The approximate round trip times are: Minimum = 0ms, Maximum = 15ms, Average = 3ms.

```
Packet Tracer PC Command Line 1.0
C:\>ping
Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target









C:\>ping FE80::2D0:97FF:FE95:2410

Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:

Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=15ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128

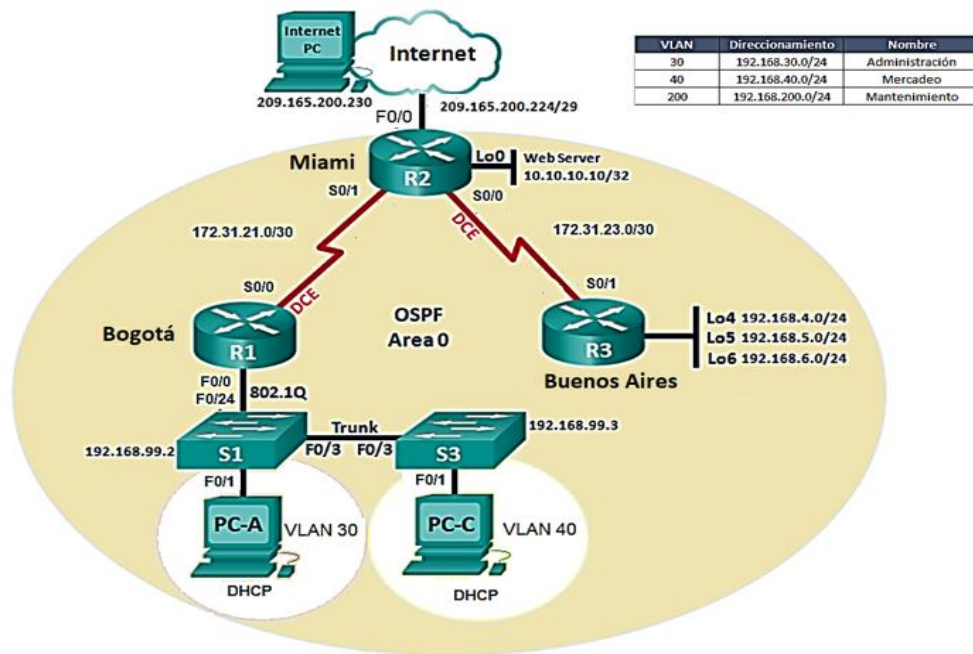
Ping statistics for FE80::2D0:97FF:FE95:2410:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 3ms

C:\>|
```

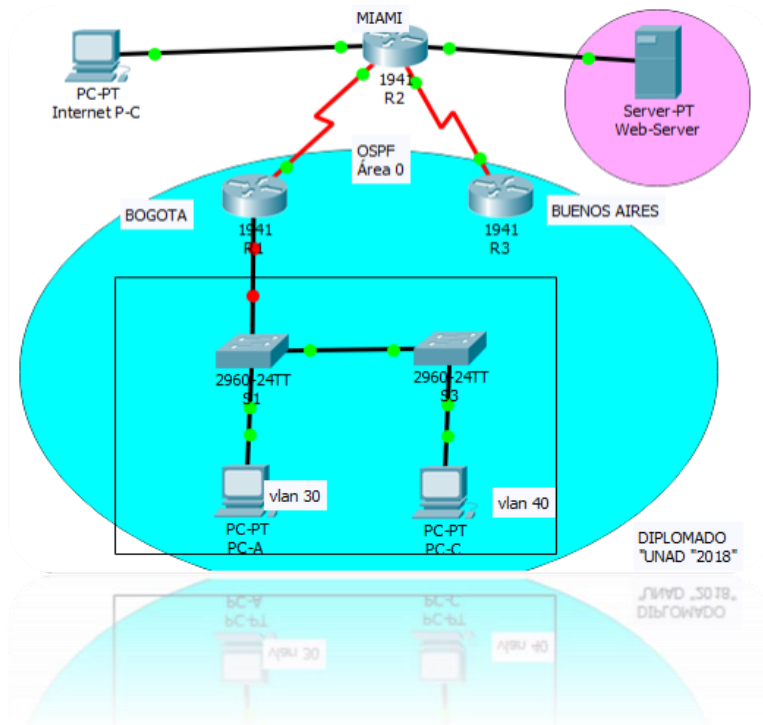
| <div> <div>Realtime</div> <div>Simulation</div> </div>                            |             |         |             |      |   |           |          |     |        |          |
|---|-------------|---------|-------------|------|---|-----------|----------|-----|--------|----------|
|   | Last Status | Source  | Destination | Type | Color   | Time(sec) | Periodic | Num | Edit   | Delete   |
|  | Successful  | PC31    | Server0     | ICMP |  | 0.000     | N        | 0   | (edit) | (delete) |
|  | Successful  | PC31    | R3          | ICMP |  | 0.000     | N        | 1   | (edit) | (delete) |
|  | Successful  | PC31    | ISP         | ICMP |  | 0.000     | N        | 2   | (edit) | (delete) |
|  | Successful  | Server0 | ISP         | ICMP |  | 0.000     | N        | 3   | (edit) | (delete) |

## 7. ESCENARIO 2

**Escenario 2:** Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.



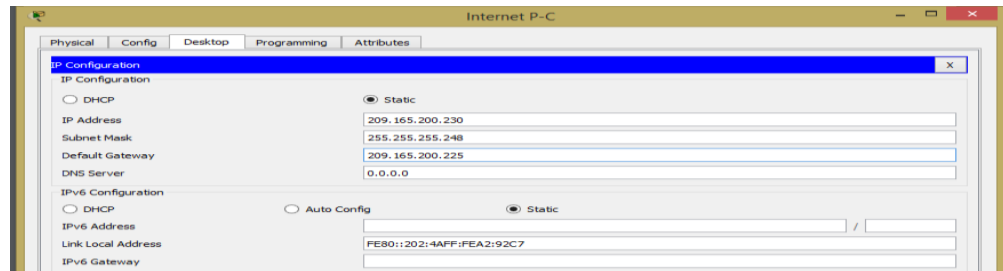
## Escenario 2



7.1 Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.

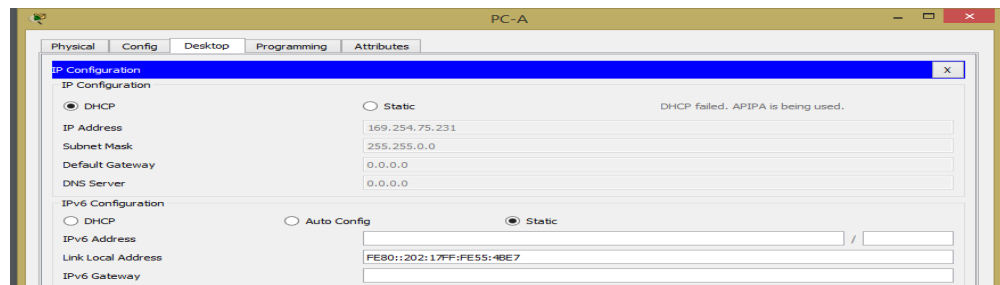
### Para Internet PC

#### Ilustración 1



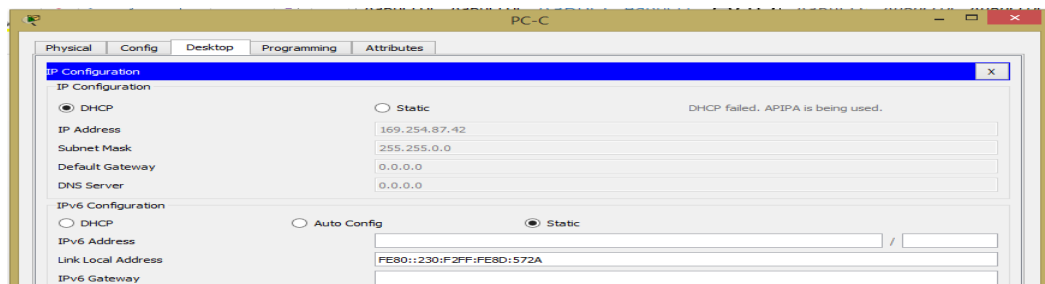
### Para PC-A

#### Ilustración 2. DHCP del PC-A



### Para PC-C

#### Ilustración 13. DHCP del PC-C



### **R1-Bogotá**

```
en
config t
interface serial 0/0/0
description connection to R2
ip address 172.31.21.1 255.255.255.252
no shut
exit
ipv6 route ::/0 s0/0/0
```

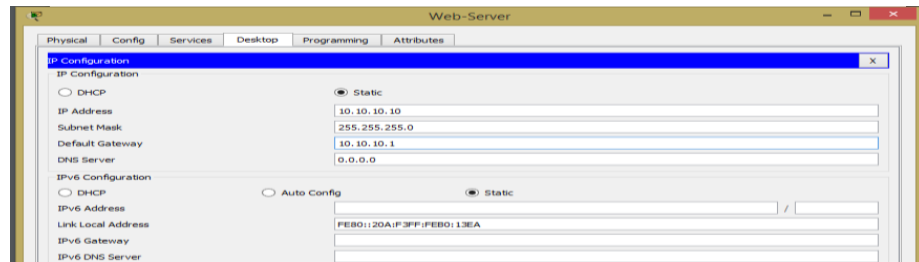
### **R2- Miami**

```
en
config t
no ip domain-lookup
hostname R2
interface serial 0/0/0
ip address 172.31.21.2 255.255.255.252
no shut
interface serial 0/0/1
ip address 172.16.31.1 255.255.255.252
no shutdown
interface gigabitEthernet 0/1
description connection to internet
ip address 209.165.200.233 255.255.255.248
no shutdown
interface gigabitEthernet 0/0
description connection to Internet
ip address 209.165.200.225 255.255.255.248
no shutdown
ipv6 route ::/0 g0/1
```



## Web Server

### Ilustración 14. Static para Web Server



## R3- Buenos Aires

```
en
config t
interface serial 0/0/1
description connection to R2
ip address 172.31.23.2 255.255.255.252
no shutdown
interface loopback4
ip address 192.168.4.1 255.255.255.0
interface loopback 5
ip address 192.168.5.1 255.255.255.0
interface loopback 6
ip address 192.168.6.1 255.255.255.0
ipv6 route ::/0 s0/0/1
```

7.2 Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:  
OSPFv2 área 0

**Tabla 1. OSPFv2 área 0**

Tabla 1. OSPFv2 área 0

| Configuration Item or Task                            | Specification |
|---|---------------|
| Router ID R1  | 1.1.1.1       |
| Router ID R2  | 5.5.5.5       |
| Router ID R3  | 8.8.8.8       |
| Configurar todas las interfaces LAN como pasivas      |               |
| Establecer el ancho de banda para enlaces seriales en | 256 Kb/s      |
| Ajustar el costo en la métrica de S0/0 a              | 9500          |

**Descripción:** Se procede a realizar la configuración del protocolo de enrutamiento OSPFv2 en cada uno de los routers que componen la red propuesta.

### R1- Bogotá

```
enable
config t
router ospf 1
router-id 1.1.1.1
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.3 area 0
network 192.168.40.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
auto-cost reference-bandwidth 9500
exit
int s0/0/0
bandwidth 256
ip ospf cost 9500
exit
```

### R2- Miami

```
en
config t
router ospf 1
```

```
router-id 5.5.5.5
network 172.31.21.0 0.0.0.3 area 0
network 172.31.23.0 0.0.0.3 area 0
network 10.10.10.0 0.0.0.255 area 0
passive-interface g0/1
auto-cost reference-bandwidth 9500
int s0/0/0
bandwidth 256
int s0/0/1
bandwidth 256
ip ospf cost 9500
exit
```

### **R3- Buenos Aires**

```
en
config t
router ospf 1
router-id 8.8.8.8
network 172.16.31.23 0.0.0.3 area 0
network 192.168.4.0 0.0.3.255 area 0
passive-interface loopback 4
passive-interface loopback 5
passive-interface loopback 6
auto-cost reference-bandwidth 9500
int s0/0/1
bandwidth 256
ip ospf cost 9500
exit
```

Verificar información de OSPF

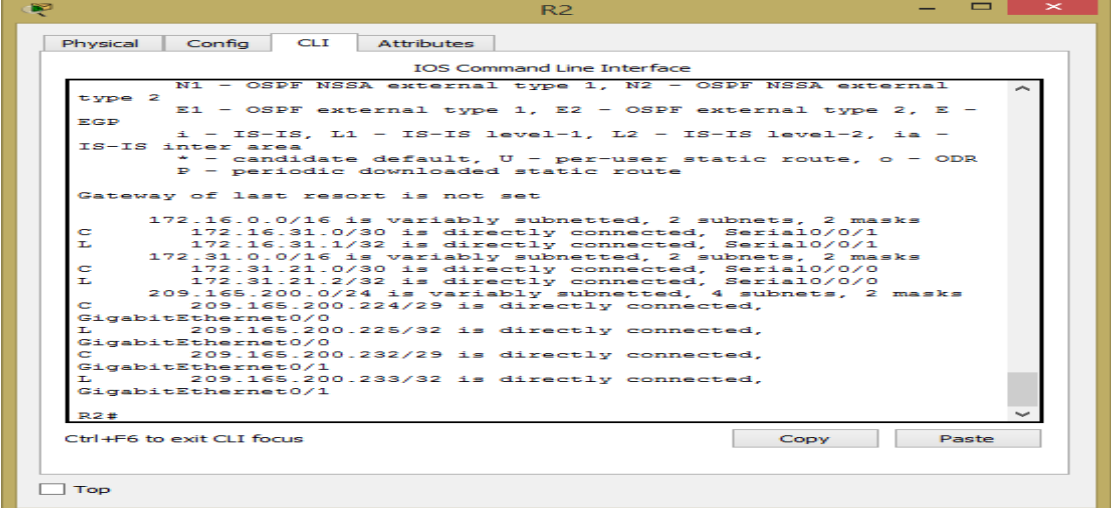
- a) Visualizar tablas de enrutamiento y routers conectados por OSPFv2
- b) Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
- c) Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

a) Visualizar tablas de enrutamiento y routers conectados por OSPFv2

**R2- Miami**

**Show ip route**

Enrutamiento y routers conectados por OSPFv2



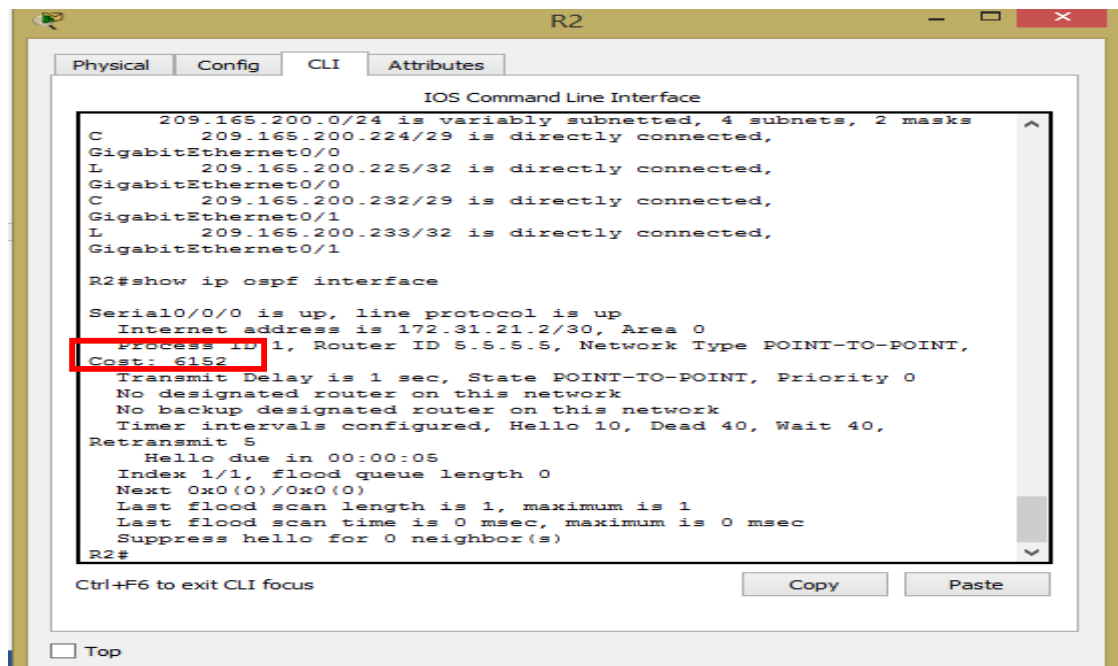
```
IOS Command Line Interface
type 2 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
EGP E1 - OSPF external type 1, E2 - OSPF external type 2, E -
IS-IS i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
C 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
L 172.16.31.0/30 is directly connected, Serial0/0/1
L 172.16.31.1/32 is directly connected, Serial0/0/1
C 172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
L 172.31.21.0/30 is directly connected, Serial0/0/0
L 172.31.21.2/32 is directly connected, Serial0/0/0
L 209.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
C 209.165.200.224/29 is directly connected,
GigabitEthernet0/0
L 209.165.200.225/32 is directly connected,
GigabitEthernet0/0
C 209.165.200.232/29 is directly connected,
GigabitEthernet0/1
L 209.165.200.233/32 is directly connected,
GigabitEthernet0/1
R2#
```

b) Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.

**R2- Miami**

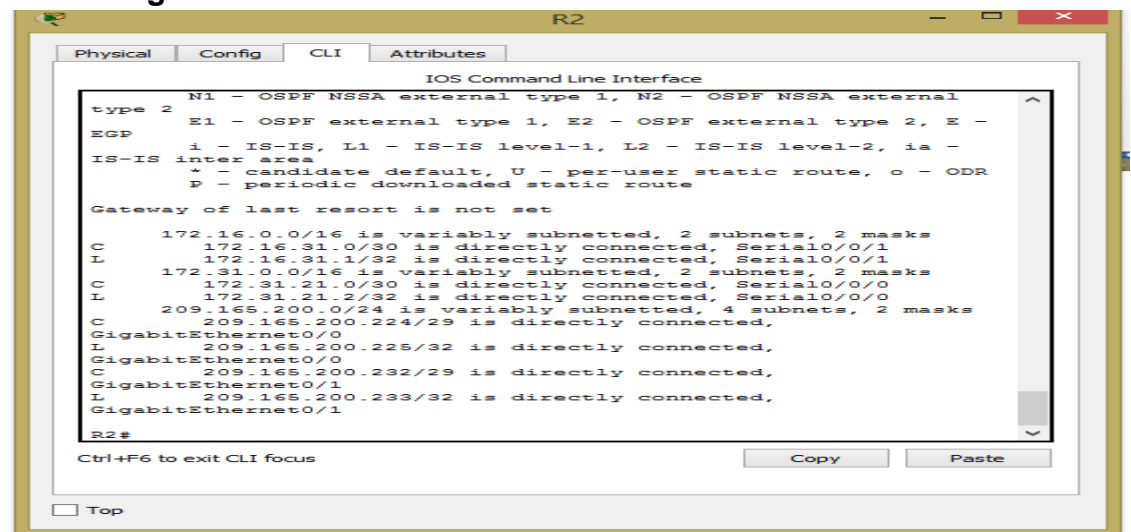
**Show ip ospf interface**

Interfaces por OSPF



- c) Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

### Interfaces configuradas en cada router



7.2 Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

**Descripción:** En el punto 1 se realizó una configuración básica de seguridad en los switches S1 y S3 en este punto se deshabilitarán los puertos del Switches que no sean utilizados.

Base de datos VLAN

| VLAN | DIRECCIONAMIENTO | NOMBRE         |
|------|------------------|----------------|
| 30   | 192.168.30.0/24  | ADMINISTRACIÓN |
| 40   | 192.168.40.0/24  | MERCADEO       |
| 200  | 192.168.200.0/24 | MANTENIMIENTO  |

Para la configuración de los puertos troncales se utiliza la VLAN 1 como VLAN Nativa. Las demás interfaces se configuran como puertos de acceso con el comando interface range.

### **Configuración VLAN - S1**

Se configuran troncales en los puertos f0/3 y f0/24 y se asigna el puerto f0/1 a la VLAN 30 Administración, según la topología

```
S1
en
config t
30
vlan 30
name Administracion
40
vlan 40
name Mercadeo
200
vlan 200
name Mantenimiento
exit
int vlan 200
interface vlan 200
ip address 192.168.99.2 255.255.255.0
no shut
exit
```

```
ip default-gateway 192.168.99.1
interface f0/3
switchport mode trunk
switchport trunk native vlan 1
interface f0/24
switchport mode trunk
switchport trunk native vlan 1
interface range f0/2, f0/4-23, g0/1-2
switch mode access
interface f0/1
switch mode access
switch access vlan 30
interface range f0/2, f0/4-23, g0/1-2
shutdown
```

### **Configuración VLAN - S3**

Se configura troncal en el puerto f0/3 y se asigna el puerto f0/1 a la VLAN 40 Mercadeo, según la topología.

```
S3
vlan 30
name Admnistracion
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
int vlan 200
ip address 192.168.99.3 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1
exit
```

## Configuración encapsulamiento - Router Bogotá

La configuración de encapsulamiento se realiza en el router Bogotá (802.1Q en subinterfaz .30, .40 y .200 – Puerto f0/0)

### R1- Bogotá

```
En
Config t
int g0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
int g0/1.40
ip address 192.168.40.1 255.255.255.0
int g0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
int g0/1.40
ip address 192.168.40.1 255.255.255.0
```

### 3 En el Switch 3 deshabilitar DNS lookup

Para realizar esto se utiliza el comando no ip domain-lookup.

```
en
config t
no ip domain-lookup
```

#### 7.3 Asignar direcciones IP a los Switches acorde a los lineamientos.

En el punto 3 se asignaron las direcciones asignadas para dos switches, y se les asignaron la dirección de administración y la dirección de gateway predeterminada. Y nuevamente se muestra esta configuración.

Teniendo en cuenta que las IP se modificaron respecto al documento pues no existe una VLAN 99 si no una VLAN 200 y si se le asignara la configuración en los lineamientos no sería correcta la comunicación.

```
S1
en
```



```
config t
interface vlan 99
ip address 192.168.99.2 255.255.255.0
no shut
exit
```

```
S3
en
config t
interface vlan 99
ip address 192.168.99.3 255.255.255.0
exit
ip default-gateway 192.168.99.1
```

7.4 Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Teniendo en cuenta como medida de seguridad se llevó a cabo desinstalar las interfaces que no se utilizan en los switches S1 y S3. Mostrando evidencia de ello y se desactivaran las interfaces no utilizadas en los routers Bogotá, Miami y Buenos Aires.

#### **S1- Desactivar interfaces no usadas**

```
en
config t
interface range f0/2, f0/4-23, g0/1-2
shutdown
```

#### **S3 - Desactivar interfaces no usadas**

```
en
config t
interface range f0/2, f0/4-23, g0/1-2
shutdown
```

#### **Router Bogotá – Desactivar interfaces no usadas**

```
Bogota(config)#int s0/0/0
Bogota(config-if)#shut
```

```
Bogota(config-if)#int s0/1/0
Bogota(config-if)#no shut
Bogota(config-if)#s0/1/1
Bogota(config-if)#shut
Bogota(config-if)#int f0/1
Bogota(config-if)# shut
```

### **Router R2 Miami – Desactivar interfaces no usadas**

```
R2(config-if)#int s0/1/0
R2(config-if)#shut
```

%LINK-5-CHANGED: Interface serial0//1/1, changed state to administratively down

```
R2(config-if)#int s0/1/1
R2(config-if)#shut
```

%LINK-5-CHANGED: Interface serial0//1/1, changed state to administratively down

### **Router R3 Buenos Aires – Desactivar interfaces no usadas**

```
BuenosAires(config)#int range f0/0/1
Buenosaires(config-if-range)#shut
BuenosAires(config-if-range)#int s0/0/0
Buenosaires(config-if)# shut
Buenosaires(config-if)#s0/1/0
BuenosAires(config-if)#shut
BuenosAires(config-if)#int s0/1/1
Bogota(config-if)# shut
```

## 7.5 Implementar DHCP and NAT for IPv4

Primero se debe elaborar los siguientes puntos 8, 9 y 10 de la prueba de habilidades.

### **R3- Buenos aires**

```
en
config t
interface loopback 4
ip address 192.168.4.1 255.255.255.0
no shutdown
exit
```

7.6 Configurar R1 como servidor DHCP para las VLANs 30 y 40.

```
en
config t
ip dhcp excluded-address 172.16.30.0
ip dhcp pool
```

7.7 Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

**Tabla 2. Reservas de direcciones IP**

|                                   |  |
|-----------------------------------|--|
| Configurar DHCP pool para VLAN 30 | Name: ADMINISTRACION<br>DNS-Server: 10.10.10.11<br>Domain-Name: ccna-unad.com<br>Establecer default gateway. |
| Configurar DHCP pool para VLAN 40 | Name: MERCADEO<br>DNS-Server: 10.10.10.11<br>Domain-Name: ccna-unad.com<br>Establecer default gateway.       |

**R1- Bogotá**

```
enable
config t
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.40.1 192.168.40.30
ip dhcp pool ADMINISTRACION
dns-server 10.10.10.11
default-router 192.168.30.1
network 192.168.30.1 255.255.255.0
ip dhcp pool MERCADEO
dns-server 10.10.10.11
default-router 192.168.40.1
network 192.168.40.1 255.255.255.0
```

7.8 Configurar NAT en R2 para permitir que los hosts puedan salir a internet

**ip http server Este comando no es soportado**

```
config t
```

```
ip http server (Este comando no es soportado )  
ip nat inside source static 10.10.10.10 209.165.200.229  
interface g0/0  
ip nat outside  
interface g0/1  
ip nat inside
```

7.9 Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

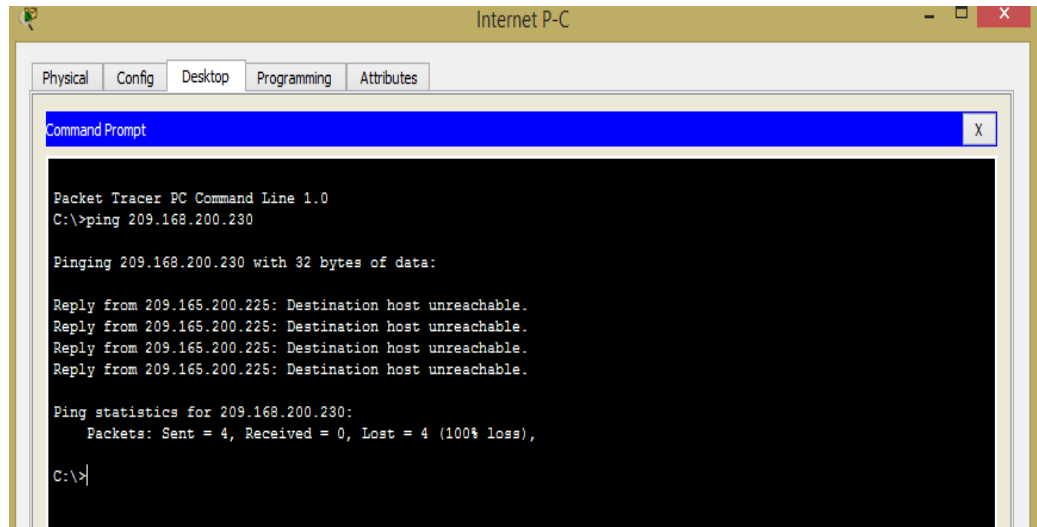
```
en  
config t  
access-list 1 permit 169.254.211.2 255.255.0.0  
interface serial 0/0/0  
access-list 1 permit 169.254.220.39 255.255.0.0  
interface serial 0/0/0
```

7.10 Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

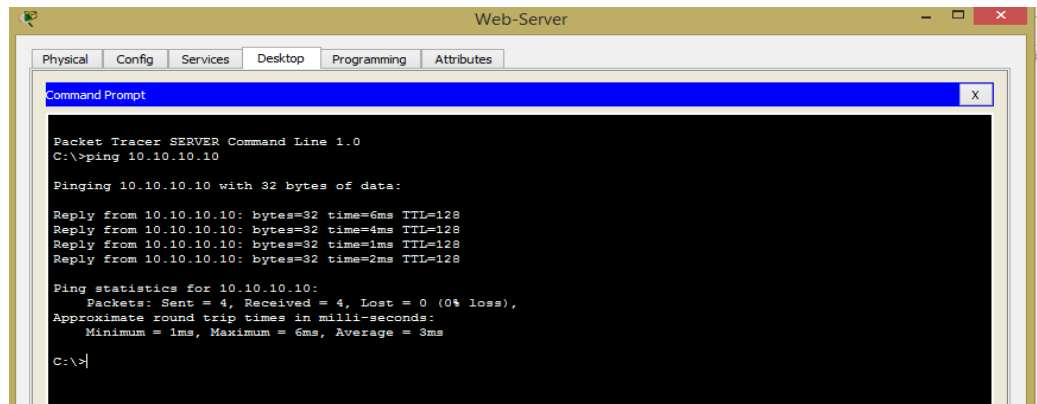
```
en  
config t  
access-list 101 permit icmp any any echo-reply  
interface g0/0  
ip access-group 101 in  
ip access-group 101 out
```

7.11 Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

## Ping Internet PC



## Ping Web Server



## 8. CONCLUSIONES

- Se realiza la configuración correspondiente para el escenario 1 y cada uno de sus dispositivos, donde se logra diseñar una topología.
- Dentro del escenario 1 se realiza la configuración de la topología de manera exitosa basados en las VLAN y puertos asociados en la tabla.
- Se logra implementar el enmascaramiento, NAT de los distintos dispositivos.
- Se aplicaron los conocimientos adquiridos para la Configuración de protocolos que permiten interconectar cada uno de los dispositivos.
- Se realiza las diferentes configuraciones de routing y Vlan, las cuales incluyen direccionamiento IP entre troncales y subinterfaces.
- Los diferentes escenarios se comprende de una manera más clara cuál es la funcionalidad concreta del protocolo DHCP.
- Se lleva a cabo la habilitación del protocolo DHCP sobre un servidor que cuenta con una administración centralizada de cada una de las diferentes direcciones IP que se encuentran dentro de la topología establecida.
- El uso de Redes VLAN para enrutar redes, da un mayor rendimiento y capacidad de administración
- Se analizó la arquitectura propuesta con el fin de implementarla sobre el software de simulación Packet Tracer

## 9. REFERENCIAS BIBLIOGRAFICAS

- CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: <https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>
- Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live>
  - CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>
  - CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>
  - CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>
  - CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>
  - CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>